Spoof Proof

Garvit Agarwal, Sunil Maggu
Department of Information Technology, Maharaja Agrasen Institute of Technology, Rohini, Delhi 86.

***Abstract*—A complete tool that checks and prevents DNS as well as ARP spoofing in home routers. We plan to deliver a tool that automizes the process of detecting DNS and ARP SPOOFING in home routers. Also, the tool will secure the router to prevent any further attacks by creating a file containing the list of mac address(s) of the attackers. DNS Spoofing can be prevented by educating people thus our tool will also be providing tips on how to be secure using deep learning.**

I. INTRODUCTION

This article suggests a methodology to provide a working proof of defending servers /systems /networks against attackers in the exclusive range of spoofing attacks. The variety of spoofing attacks being included is among DNS and ARP spoofing. This project not only safeguards it against these attacks but also provide a long-term benefit which would eradicate the very existence of systems that are being used for such attacks.

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber-attack such as an advanced persistent threat or a man-in-the-middle attack.

Successful attacks on organizations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organization's public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.

Spoofing can be applied to a number of communication methods and employ various levels of technical know-how. Spoofing can be used to carry out phishing attacks, which are scams to gain sensitive information from individuals or organizations.

The objective of our work is to:

- Make system robust.
- Blacklist malicious systems.
- Understanding attack patterns.
- Eradicate ARP Spoofing attacks.
- Eradicate DNS Spoofing attacks.

II. RESEARCH STUDY

Now it is the time to articulate the research work with previously gained and learned knowledge. These include some of the basic terminology required to solve the problem statement. These also include certain definitions which help in understanding the concept of DNS spoofing more clearly and its prevention even more effectively.

A. DNS (Domain Name System)

DNS stands for Domain Name System. A domain is a unique string associated with an IP address. An IP address is a string of numbers used to identify a computer or resource on a network or internet. The Domain Name System (DNS) is a network of directories on the internet used to resolve host names (e.g., www.gingernameclub.com) into machine-readable IP addresses (e.g., 192.168.106.81).

DNS Traffic Essentiality

The domain name system (DNS) is an essential component of the Internet used to associate symbolic host names with numeric IP addresses. Internet service providers often perceive the DNS as a core system they must keep up and running as their customers rely on it, but being it a service that does not bring revenues, they do not usually invest much on it. The consequence is that ISP's DNS servers are sometimes slowing responses [1], and this has opened the market to public DNS servers such as OpenDNS and Google Public DNS .Beside premium services, such public DNSes offer the service at no cost while making revenues through advertisements, web traffic redirection and mining of DNS data. Although the DNS is perceived as a critical infrastructure [2], all publicly available DNS traffic monitoring tools [3] [4] focus only on aggregate values such as the type and number of queries received by a DNS server [5]. Research and academia have focused on DNS for the purpose of identifying malicious activities [6] [7] [8], managing large DNS infrastructures [9],understanding how DNS server selection and caching works in reality [10] [11], and modeling its infrastructure in order to predict how DNS traffic will change under specific conditions[12]. The lack of a specific model for DNS traffic has been the motivation for this work [13] [14]. As explained later on this paper, such model can be of fundamental importance for understanding patterns, trends and interests in the Internet without having to monitor large amount of (often encrypted) traffic on multi-Gbit backbones.

So to understand clearly,A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or

translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols.

DNS Records Caching [15]

Each record has a Time to Live (TTL) [16], that can range from 0 (i.e., no cache) to days or weeks. It determines for how long the given response record can be kept in cache. The consequence of the DNS caching architecture is that DNS record updates do not propagate immediately in the network until cached records expire. Record caching is a pretty complex mechanism [16] as all DNS records used in the resolution process do not necessarily have uniform TTL values. Supposing that a DNS resolver starts with an empty cache, the resolution of www.corriere.it, its cache at the end of the iterative resolution will be populated by over 290 records. The record for www.corriere.it lasts 600 seconds in cache, shorter than the name server record of corriere.it (it lasts 10800 seconds) and shorter than the name server record for .it (it last 172800 seconds). So if the same record www.corriere.it is requested after 700 seconds, the resolver will no longer have the IP in cache as the record expired in the meantime, but will still cache the NS record for corriere.it. The resolver will contact again ".it" DNS servers only when the NS record for corriere.it has expired.

DNS Functionality

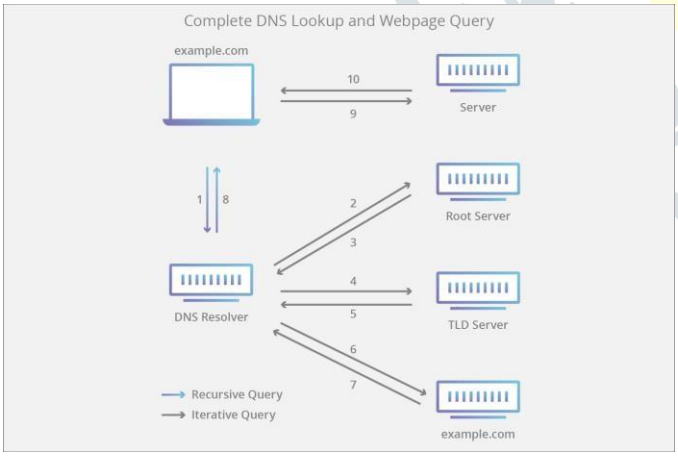

Fig 1

The Domain Name System (DNS)[16] is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

B. ARP (Address Resolution Protocol)

ARP [17] (Address Resolution Protocol) is an IP address into physical address Protocol. There are two mapping methods from IP address to physical address: tabular and non-tabular. In particular, it is the network layer (equivalent to the OSI structure of the network layer) IP address resolution for the network interface layer (equivalent to OSI Structure of the data link layer) of the MAC address. ARP packet format shown in the Table above.

Attribute	Size
destination address	6byte
source address	2byte
ARP request/replay	2byte
type	28byte

ARP works like this: First, the source host will send out a destination IP address of the Ethernet Broadcast packets, and then the destination host will answer a packet that contains both the IP address and the MAC address. So the source host will be able to obtain the destination host IP/MAC mapping, and this correspondence into their own ARP cache. When the two sides need to communicate the next communication, you can directly remove the correspondence from the ARP cache, omitting unnecessary ARP requests and responses. Like this is shown in Figure 1.

As shown in Figure 1, suppose there are three hosts and two gateways in the two network segments. Assume that host A wants to communicate with the host B communication, if the host B and their own in the same segment, the host A will check whether their ARP cache host B IP / MAC mapping; if not in the same network segment, it will send ARP to all hosts Request the broadcast, the request to obtain the host B corresponding MAC address. Theoretically only host B will respond to this ARP request, and respond to an ARP response packet, the response packet contains the host B corresponding to the MAC address. Through such a communication, the host A to obtain the host B's MAC address, and the host B's IP / MAC mapping saved in their own ARP cache table. When Host A and Host B communicate with each other again, they can find the IP / MAC correspondence in their ARP cache tables. This entry is removed from the ARP cache table until both parties have stopped communicating for an aging time

When an address resolution packet is received, the receiving Ethernet module gives the packet to the Address Resolution module which goes through an algorithm similar to the following. Negative conditionals indicate an end of processing and a discarding of the packet.

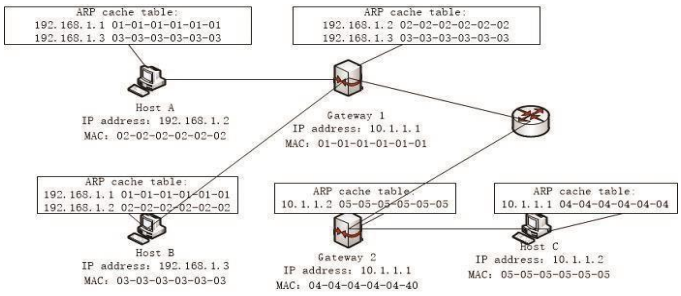

Fig 2

MATH behind ARP aging

Formula 1. describes the aging mechanism of the ARP cache table, where T represents the ARP cache table, item represents entries in the cache table, age represents the aging time of the item, Timeout represents the maximum aging time specified by the system, and Remove In addition to the corresponding entry. If a row in the table is not used again during the aging time, it is deleted. This design can greatly reduce the ARP cache table system overhead, while speeding up the query.

(item T)&(item.age Timeout) T Remove(item)

C. ARP Spoofing Detection, Prevention and Protection

- Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
- Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. Trust relationships rely only on IP addresses for authentication, making it significantly easier for attackers to run ARP spoofing attacks when they are in place.
- Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
- Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

D. ARP Spoofing Attacks

The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

- Denial-of-service attacks: DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.
- Session hijacking: Session hijacking attacks can use ARP spoofing to steal session IDs, granting attackers access to private systems and data.
- Man-in-the-middle attacks: MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

E. DNS spoofing mitigation using domain name server security (DNSSEC)

DNS is an unencrypted protocol, making it easy to intercept traffic with spoofing. What's more, DNS servers do not validate the IP addresses to which they are redirecting traffic.

DNSSEC is a protocol designed to secure your DNS by adding additional methods of verification. The protocol creates a unique cryptographic signature stored alongside your other DNS records, e.g., A record and CNAME. This signature is then used by your DNS resolver to authenticate a DNS response, ensuring that the record wasn't tampered with.

III. SCOPE OFTHE PROJECT

The project majorly focuses on the defense against the spoofing attacks. To battle these attacks, the project consist of four different operations, with two options and two modes.

These operations are responsivble for successful detection, prevention and protection from Spoofing attaks. These modes of operations are well defined as below:

Option 1: Defensive Option

Defensive mode is the ultimate strategy for the user to defend the servers at all times by not letting the attacker into the servers. The defensive mode works in the gateway layer of the network and wouldn't allow any changes in the network layer of the network.

Option 2: Offensive Option

The ARP spoofer will be immediately be disconnected from the server even if the attacker is already present in the network already.

Mode 1: Active Mode

Active mode uses active scanning method. Recommended while the system is idle most of the time. During an active scan, the client radio transmits a probe request and listens for a probe response from an AP.

Mode 2: Passive Mode

With a passive scan, the client radio listens on each channel

for beacons sent periodically by an AP. A passive scan generally takes more time, since the client must listen and wait for a beacon

Reset Option

Reset network interface card and network manager (suggested to use after operating the offensive mode).

MAC Decoder:

Furthermore, a series of research is pending on the account of deep learning that will be used to study the pattern of the attacks of the so instated attacks that are being consistent to networks all around the world.

IV. RESULTS

The detection of any attacker using spoofing as his weapon was absolute and the accuracy of detecting such an act was 100%. There were no clear drawbacks or showstoppers that would prevent Spoof Proof from functioning.

Such a detection of attack is exhibited in Fig 2, where an attack with MAC address '88:3e:8e:c5:db:cf' is caught spoofing on the victim machine.

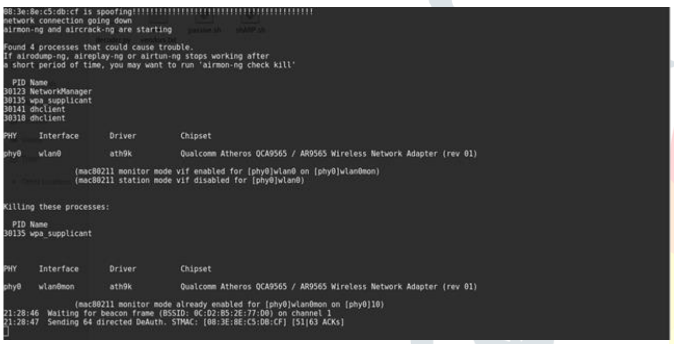

Fig 2

The core functioning of the working application is depicted in Fig 3 where we are opting to use Spoof Proof on the wireless local interface (wlan0).

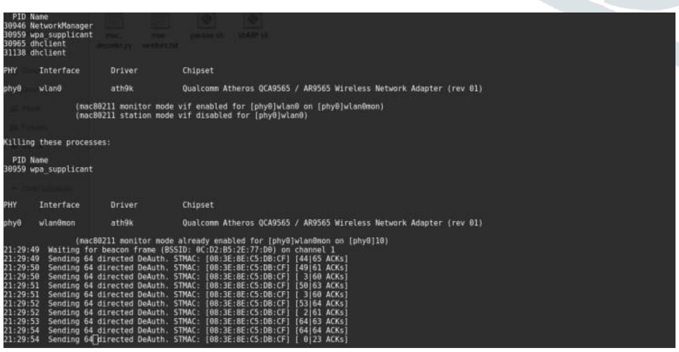

Fig 3

V. CONCLUSION

The initial problem of protecting against spoofing attacks, namely ARP spoofing and DNS spoofing was achieved at the initial stage of project. There were four mode of operations which were employed to fend off attackers, namely Defensive-Active mode, Defensive-passive mode, Offensive-active mode and Offensive-passive mode.

Furthermore, the attacker was immediately disconnected and the identity of the attacker was revealed, thus providing us the physical address (MAC address) and the local ip. This would help us in detecting what traffic was utilized by the attacker and what data he might have stolen us during the time he was present in the network. After some deep learning classification on the information of the packets of the attackers, we could find a pattern as to what information would be vulnerable for the user, and what all measures need to be taken to safeguard it.

REFERENCES

[1] G. R. Corporation, "Domain name speed benchmark," 2012. [Online]. Available: https://www.grc.com/dns/benchmark.htm

[2] E. Casalicchio and I. N. Favino, "The 1st workshop on dns health and security," 2012. [Online]. Available: http://www.gcsec.org/sites/default/files/files/dnseasy2011.pdf

[3] D. Plonka and P. Barford, "Context-aware clustering of dns query traffic," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, ser. IMC '08. New York, NY, USA: ACM, 2008.

[4] T. M. Factory, "dnstop and dsc tools," 2006. [Online]. Available: http://dns.measurement-factory.com/tools/

[5] E. Osterweil, D. McPherson, S. DiBenedetto, C. Papadopoulos, and D. Massey, "Behavior of dns' top talkers, a .com/.net view," in *Proceedings of the 13th international conference on Passive and Active Measurement*. Berlin, Heidelberg: Springer-Verlag, 2012.

[6] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a dynamic reputation system for dns," *9th Usenix Security Symposium*, 2010.

[7] A. Berger and E. Natale, "Assessing the real-world dynamics of dns," in *Proceedings of the 4th international conference on Traffic Monitoring and Analysis*, ser. TMA'12. Berlin, Heidelberg: Springer-Verlag, 2012.

[8] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on*, 2009.

[9] C.-S. Chen, S.-S. Tseng, and C.-L. Liu, "A unifying framework for intelligent dns management," *International Journal of HumanComputer Studies*, vol. 58, no. 4, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1071581903000120

[10] D. Wessels, M. Fomenkov, N. Brownlee, and k. claffy, "Measurements and laboratory simulations of the upper dns hierarchy," in *Passive and Active Network Measurement*, ser. Lecture Notes in Computer Science, C. Barakat and I. Pratt, Eds. Springer Berlin Heidelberg, 2004, vol. 3015.

[11] J. S. Otto, M. A. Sanchez, J. P. Rula, and F. E. Bustamante,´ "Content delivery and the natural evolution of dns: remote dns trends, performance issues and alternative solutions," in *Proceedings of the 2012 ACM conference on Internet measurement conference*, ser. IMC '12. New York, NY, USA: ACM, 2012, pp. 523–536. [Online]. Available: http://doi.acm.org/10.1145/2398776.2398831

[12] A. J. Yakup Ko and B. Gijsen, "A global reference model of the dns," *Proceedings of DNS EASY 2011 Workshop*, 2012.

[13] J. M. Agosta, J. Chandrashekar, M. Crovella, N. Taft, and D. Ting, "Mixture Models of Endhost Network Traffic," *ArXiv e-prints*, Dec. 2012.

[14] N. Brownlee and K. Claffy, "Understanding internet traffic streams: dragonflies and tortoises," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 110 – 117, oct 2002.

[15] Luca Deri, Simone Mainardi, Maurizio Martinelli, "Graph Theoretical Models of DNS Traffic," Department of Information Engineering (IET), University of Pisa, Pisa, Italy.

[16] https://www.cloudflare.com/learning/dns/what-is-dns/

[17] AIP Conference Proceedings 1820, 090019 (2017);https://doi.org/10.1063/1.4977403Published Online: 13 March